

## GENERATOR FOR TILFÆLDIGE TAL

H. Isaksson

TFL

Med henblik på anvendelsen af den danske elektroniske cifferregnemaskine DASK til løsning af trafikteoretiske problemer har Teleteknisk Forskningslaboratorium udviklet en generator for tilfældige tal. I artiklen gives en beskrivelse af generatoren og dens virkemåde samt et eksempel på dens anvendelse. Generatoren, der udnytter støjspændingen fra en diode, kan frembringe 5000 binære cifre pr. sekund. De tilfældige tal har været underkastet en række statistiske prøver for tilfældighed, hvilke alle gav tilfredsstillende resultater.

DK 681.14 — 523.8

## Indledning

Den trafikmæssige dimensionering af telefoncentraler og ledningsbundter kan foretages på et rent matematisk grundlag, fordi erfaringen har vist, at samtalehyppighed og -varighed følger bestemte statistiske fordelinger. På dette grundlag er man i stand til at opstille en stokastisk model af et hvilket som helst foreliggende koblingsproblem. Ved hjælp af den klassiske sandsynlighedsregning overføres dette problem i sandsynligheder til et problem i funktionelle ligninger, hvis løsning er et rent matematisk problem. Udviklingen af denne metode vil kun ganske kort blive skitseret her, idet der henvises til tidligere artikler om emnet. (Se f. eks. litt. 1. Følgende oversigt er et uddrag af nævnte artikel).

Et matematisk grundlag til beregning af afvisningen i telefonsystemer baseret på sandsynlighedsregning blev for første gang opstillet af A. K. Erlang. Han udledte den fundamentale *B*-formel, hvor man bestemmer afvisningen for simple organgrupper, d. v. s. grupper hvis organer (ledninger eller vælgere) samarbejder således, at ethvert opkald til gruppen kan søge ind på et vilkårligt af de ledige organer.

I moderne telefonsystemer forekommer imidlertid talrige tilfælde, hvor samarbejdet mellem de forskellige organer i en gruppe er mindre fuldkomment, idet et vilkårligt opkald til gruppen kun har adgang til visse af gruppens organer. Dette gælder f. eks. for afgående ledningsbundter fra vælgergrupper, når trafikken kræver et ledningsantal, der er større end vælgernes kontaktantal, hvorfor man fordeler ledningerne over vælgerne i en såkaldt gradering. Med en udvidet betydning af dette udtryk kan en række problemer med begrænset adgang til en organgruppe sammenfattes under betegnelsen graderingsproblemer.

Erlang har undersøgt et teoretisk set særligt simpelt graderingsproblem og opstillet en eksakt formel for beregning af afvisningen, den såkaldte

»ideelle graderingsformel«. Her betragtes et ledningsbundt med  $n$  ledninger, der modtager totaltrafikken  $A$  fra vælgere med  $k$  kontakter, således at opkaldene fra en bestemt vælger har adgang til  $k$  bestemte af de  $n$  ledninger, og det antages, at trafikken kan regnes fuldstændig tilfældigt fordelt over de  $n$  ledninger. Sandsynligheden for afvisning bestemmes da ved Erlangs ideelle graderingsformel.

Det almindelige graderingssystem, som er meget hyppigt anvendt i automatiske telefonsystemer, er mere kompliceret. Man arbejder her med sær- og fællesledninger som vist på fig. 1. Her er 9 organer fordelt over 2 vælgergrupper. Hver

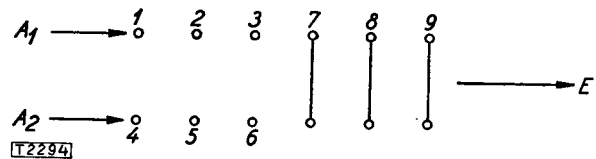


Fig. 1. Gradering.

vælgergruppe har 3 individuelle organer 1—3 og 4—6, medens de 3 resterende organer 7—9 er fælles for de to vælgergrupper. Trafikken på de to grupper er henholdsvis  $A_1$  og  $A_2$  Erlang. I 1936 offentliggjorde C. Palm resultaterne af en eksakt beregning af nogle simple graderinger af denne type, men formlerne er ikke velegnede for numerisk beregning. I de fleste tilfælde anvendes derfor en approksimativ metode, der er fremsat af O'Dell, selvom approksimationen er ret grov. Ved mere komplicerede koblinger bliver vanskelighederne selvsagt større, og følgerne af indførte tilnærmelser mere uoverskuelige. Det er derfor rimeligt at søge andre veje ved løsning af graderingsproblemer.

En naturlig fremgangsmåde ville være at studere en kunstig model af det foreliggende problem, og denne metode, den såkaldte Monte Carlo metode, har også været anvendt i en del tilfælde. Den enkleste form for en sådan kunstig model finder vi i de såkaldte analogiregnermaskiner. Her kan

det enkelte organ i en gruppe f. eks. være repræsenteret ved en monostabil multivibrator (se senere), hvis omslagstid svarer til holdetiden. Ved at sammenkoble organerne på forskellig vis, således at adgangen til det enkelte organ er betinget af ét eller flere af de øvrige organers tilstand, kan man arrangere afsøgningen efter det ønskede princip. Som tidligere nævnt, kan man forudsætte, at opkaldene er tilfældigt fordelt, d. v. s. intervallerne mellem opkaldene er uafhængige af både tiden og tidspunkterne for de forudgående opkalds indtræffen. Til at simulere opkaldene i den kunstige model kræves følgelig en række tilfældige tal, som f. eks. kan angive længden af intervallerne mellem opkaldene eller tidspunkterne for opkaldenes indtræffen. Analogiregnemaskiner har imidlertid en væsentlig ulempe, idet de ifølge deres natur må bygges til løsning af en bestemt type opgaver og kun vanskeligt lader sig anvende ved andre problemstillinger.

Ved udviklingen af de moderne elektroniske cifferregnemaskiner er der skabt mulighed for at behandle alle typer af opgaver på samme maskine. Som et eksempel på anvendelsen af cifferregnemaskiner til graderingsberegninger vil der i det følgende blive vist, hvorledes man har udført en graderingsberegning på den svenske elektronregnemaskine BESK (litt. 2).

Den undersøgte gradering er den på fig. 1 viste. Der forudsættes ordnet afsøgning, eksponentielt fordelte intervaller mellem successive opkald, hvilket svarer til, at opkaldene er Poissonfordelte, og konstante holdetider. Tidsenheden vælges således, at holdetiden = 1. Til hvert organ hører to hukommelsesceller i regnemaskinens »lager«, én til tælling af de opkald, som organet modtager, og én til angivelse af det tidspunkt, hvorpå det pågældende organ bliver ledigt. Opkald, som afvises, fordi alle organer i en vælgergruppe er optaget, tælles af en tæller  $E$ , der er fælles for de to vælgergrupper. Desuden optælles den totale trafik fra hver af de to indgange  $A_1$  og  $A_2$ .

Lad  $P_1, P_2, P_3, \dots$  og  $R_1, R_2, R_3, \dots$  være to rækker tilfældige tal, hvor

$$0 < P < 1 \text{ og } 0 < R < 1.$$

Intervallerne mellem opkaldene fra  $A_1$  vil være

$$-\frac{1}{A_1} \ln P_1, \quad -\frac{1}{A_1} \ln P_2, \quad -\frac{1}{A_1} \ln P_3, \dots$$

og tilsvarende for opkaldene fra  $A_2$

$$-\frac{1}{A_2} \ln R_1, \quad -\frac{1}{A_2} \ln R_2, \quad -\frac{1}{A_2} \ln R_3, \dots$$

Intervallerne bliver herved positive tal mellem 0 og  $+\infty$ , som er eksponentielt fordelte, når tallene  $P$  og  $R$  er rektangulært fordelte tilfældige tal mellem 0 og 1. (I den rektangulære fordeling forekommer alle de mulige udfald lige hyppigt).

Det sidste opkald  $N_1$  fra  $A_1$  vil da være sket til tiden

$$t_{A_1} = \frac{1}{A_1} \sum_{v=1}^{N_1} -\ln P_v$$

Ligeledes er sidste opkald  $N_2$  fra  $A_2$  sket på tidspunktet

$$t_{A_2} = \frac{1}{A_2} \sum_{v=1}^{N_2} -\ln R_v$$

Hver gang to nye tilfældige tal  $P$  og  $R$  tilføres regnemaskinen, dannes  $t_{A_1}$  og  $t_{A_2}$ .

Tilfældet  $t_{A_1} < t_{A_2}$  tolkes som et opkald fra  $A_1$  til tiden  $t_{A_1}$ .

Tilfældet  $t_{A_2} < t_{A_1}$  tolkes som et opkald fra  $A_2$  til tiden  $t_{A_2}$ .

Der vil på denne måde kun komme et opkald fra den ene af kilderne  $A_1$  og  $A_2$ , hver gang der er tilført 2 tilfældige tal. På samme måde forøges kun den ene  $t_A$ -værdi, svarende til den vælgergruppe, som modtager et opkald.

Organernes anden hukommelsescelle indeholder størrelsen  $t_D = t_A + 1$ , som angiver, hvornår organet bliver ledigt (holdetiden = 1). For hvert opkald, d. v. s. for hver ny  $t_A$ -værdi, sammenlignes  $t_A$  med  $t_D$ -værdien for det første organ i den pågældende vælgergruppe. Hvis  $t_A < t_D$ , afvises opkaldet og videreføres til det næste organ i gruppen. Hvis et organ findes ledigt, d. v. s. hvis  $t_A > t_D$ , registreres et opkald i organets ene hukommelsescelle, og en ny  $t_D$ -værdi, nemlig  $t_A + 1$ , indsættes i den anden hukommelsescelle.

Denne proces fortsættes, indtil man har opnået det ønskede antal opkald til graderingen. Antallet af opkald fra  $A_1$  og  $A_2$ , antallet af opkald modtaget af hvert organ, og antallet af afviste opkald  $E$  er det søgte forsøgsresultat. Et forsøg af denne art med  $2^{16} = 65\,536$  opkald blev udført på BESK på ca. 15 min.

Ved at indføre en tredje serie tilfældige tal til bestemmelse af holdetiderne kan den samme metode benyttes til forsøg med eksponentielt for-

delte holdetider. I øvrigt kan man med denne metode udføre forsøg med en vilkårlig fordeling af holdetiderne og intervallerne mellem opkaldene. Hvis de tilfældige tal, som står til rådighed, følger den rektangulære fordeling, kan man nemlig transformere denne over i en hvilken som helst anden fordeling efter samme princip, som blev anvendt i ovenstående tilfælde, hvor vi dannede en eksponentielt fordelt stokastisk variabel ud fra en rektangulært fordelt variabel. Med den viste opstilling kan man ligeledes ændre det princip, hvorefter afsøgningen skal foregå.

(Foruden den ovenfor refererede publikation litt. 2, er der offentliggjort endnu en artikel vedrørende en serie Monte Carlo forsøg på telefonsystemer udført på BESK: B. Wallström: Artificial Traffic Trials on a Two-Stage Link System Using a Digital Computer. Foredrag holdt på The International Teletraffic Congress, Haag 7.—11. juli 1958).

Ved at benytte Monte Carlo metoden undgår man de fejl, som bliver indført ved brug af de matematiske metoder, hvor man foretager tilnærmelser og simplifikationer. Den usikkerhed, som opstår, når man benytter Monte Carlo metoden, kan bestemmes ved hjælp af sandsynlighedsregningen og afhænger i øvrigt kun af, hvor stort det benyttede materiale er. I det ovenfor viste graderingseksempel aftager usikkerheden (spredningen) med kvadratroden af antallet af opkald ( $A_1 + A_2$ ). Hvis man ønsker lille usikkerhed på resultatet, betyder det, at man skal bruge mange opkald, d. v. s. mange tilfældige tal. Ved anvendelse af elektroniske cifferregnemaskiner, som arbejder med store hastigheder, er man i stand til at bearbejde et meget stort materiale på en relativ kort tid, under forudsætning af at de tilfældige tal kan fremskaffes tilstrækkeligt hurtigt og i tilstrækkelige mængder.

I det følgende afsnit gives en oversigt over forskellige metoder til fremstilling af tilfældige tal.

#### *Metoder til fremstilling af tilfældige tal*

De klassiske metoder til fremstilling af tilfældige tal er af rent mekanisk art, som eksempel kan nævnes terningkast, møntkast, roulette o. s. v. På grundlag af disse metoder har man udarbejdet tabeller over tilfældige tal, som til mange formål, f. eks. stikprøveudtagning, er fuldt tilstrækkelige, men til brug ved Monte Carlo metoden i forbindelse med elektroniske regnemaskiner er tabellerne upraktiske. Vanskeligheden består i at tilføre maskinen de tilfældige tal hurtigt nok, idet

der ikke forefindes nogen indlæsningsmetode, som kan holde trit med maskinens arbejdstempo. Man kunne tænke sig den mulighed at opbevare tallene i regnemaskinens lager og hente dem der, når de skulle bruges, men da der til mange formål er brug for talmængder af størrelsesordenen  $10^6$ — $10^7$  binære tal (se senere), vil denne løsning kræve alt for stor lagerplads. Til sammenligning kan nævnes, at den samlede lagerkapacitet i den danske elektronregnemaskine DASK er på ca.  $40 \times 10^4$  binære tal. Man er derfor nødt til at fremstille tallene, efterhånden som de skal bruges.

De metoder til fremstilling af tilfældige tal, som har mulighed for at komme i betragtning, kan principielt opdeles i to grupper: de matematiske og de fysiske metoder.

Matematisk fremstilling af tilfældige tal er baseret på den erfaring, at man ved at gentage nogle enkle regneoperationer kan frembringe en talrække, hvis led med god tilnærmelse udgør en serie tilfældige tal. Disse tal er ifølge deres natur reproducerbare, hvilket kan være en fordel. Man er således i stand til nøje at spore virkningen af en ændring f. eks. i en gradering, da forsøgsbetingelserne i øvrigt kan holdes uændrede. Der vil imidlertid uundgåeligt være en periodicitet i de matematisk fremstillede tal, d. v. s. man kan kun fremstille en endelig mængde tal, som tilfredsstiller kravene om tilfældighed.

Ved fysiske metoder til fremstilling af tilfældige tal udnytter man fænomener i naturen, som har tilfældig karakter. Alle atomare processer har et tilfældigt forløb for de enkelte partiklers vedkommende; som eksempel kan nævnes radioaktiv sønderdeling af atomkerner eller elektroners kinetiske bevægelser. De fysisk fremstillede tilfældige tal vil i princippet være uperiodiske, d. v. s. man har mulighed for at producere et ubegrænset antal tilfældige tal. Som det blev nævnt i forbindelse med graderingseksemplet, kan man få forsøgsresultaterne med vilkårlig nøjagtighed, når man har tilstrækkelig mange tilfældige tal til rådighed. De fysisk fremstillede tilfældige tal giver derfor også mulighed for at iagttage virkningen af en lille ændring i f. eks. en gradering.

Før vi går over til at se nærmere på de forskellige metoder til fremstilling af tilfældige tal, vil det være nyttigt nøjere at specificere de krav, som skal stilles til tallene. Betingelserne er, at tallene skal være tilfældige, og at de skal fremstilles med en hastighed, der står i et rimeligt

forhold til regnemaskinens arbejdstempo, som for DASK's vedkommende er fastlagt ved, at 1 additionstid er lig med  $56 \mu s$ . Det skønnes, at en hastighed på 5000 binære tal i sekundet vil være tilfredsstillende. Tallene skal være binære, d. v. s. kun cifrene 0 og 1 forekommer, fordi de elektroniske cifferregnemaskiner arbejder i det binære talsystem.

#### *Definition af tilfældige tal*

En serie binære cifre siges at være tilfældige, når de opfylder følgende betingelser:

1. Sandsynligheden for udfaldet 0 er lig med sandsynligheden for udfaldet 1,  $P(0) = P(1) = \frac{1}{2}$ .
2. Ethvert udfald er uafhængigt af alle tidligere udfald.

Det er ret simpelt at undersøge, om en given serie tal opfylder den første betingelse. En simpel hyppighedsprøve på tallene 0 og 1 vil kunne afsløre en eventuel skævhed. Derimod er det ikke muligt at konstatere, om en række tilfældige tal opfylder den anden betingelse. Dette vil nemlig kræve en autokorrelationsundersøgelse (se f. eks. litt. 3, side 69) fortsat i det uendelige. Det er med andre ord umuligt at opstille en endegyldig prøve for tilfældighed. Man må derfor begrænse sig til at undersøge, om tallene opfylder en række betingelser, som er væsentlige ved tallenes anvendelse.

#### *Metoder til undersøgelse af tilfældige tal*

Der findes en lang række prøver til undersøgelse af tilfældige tal. Her vil blive benyttet 4 prøver angivet af Kendall og Smith (litt. 4), som almindeligvis bruges til kontrol af tabeller over tilfældige tal. De anvendte prøver er følgende:

1. Hyppighedsprøve
2. Hyppighedsprøve på grupper
3. Pokerprøve
4. Intervalprøve

I hyppighedsprøven findes fordelingen af 0 og 1, og denne sammenlignes med den teoretiske fordeling. Hyppighedsprøve på grupper foretages ved at bestemme den relative hyppighed af de  $2^n$  forskellige  $n$ -cifrede binære tal ( $2 \leq n \leq 8$ ), og resultatet vurderes ved en sammenligning med den teoretiske fordeling.

Pokerprøven udføres på grupper, der indeholder 5 på hinanden følgende 4-cifrede binære tal. Disse inddeles i 6 klasser:

AAAAA + AAAAB  
AAABB  
AAABC  
AABBC  
AABCD  
ABCDE

idet A, B, C, D og E hver kan antage værdierne 0000 til 1111, og hvor tallenes orden inden for gruppen er ligegyldig. Den første klasse er slået sammen af to undergrupper, da disse hver især har for små sandsynligheder til, at den såkaldte  $\chi^2$ -prøve (se f. eks. litt. 5 side 81) kan anvendes på dem enkeltvis.

Med intervalprøven bestemmes afstandene mellem på hinanden følgende ens 4-cifrede binære tal. Forskellige intervaller fra 0 til 46 og intervaller  $\geq 47$  tælles for hvert af de 16 forskellige 4-cifrede tal, svarende til et totalt antal klasser på  $16 \times 48 = 768$ .

For alle de nævnte prøver foretages en sammenligning mellem den teoretiske og den fundne fordeling ved hjælp af  $\chi^2$ -prøven. En serie tilfældige tal siges at falde for en prøve, når  $\chi^2$ -værdien svarer til en sandsynlighed, som ligger uden for intervallet:

$$0,025 \leq P(> \chi^2) \leq 0,975.$$

Disse grænser anvendes almindeligvis, men er i øvrigt vilkårligt fastlagte. Med dette 5 % signifikansniveau vil man i gennemsnitlig 5 % af tilfældene, ved overensstemmelse mellem den eksperimentelle og den teoretiske fordeling, drage den fejlslutning at kassere en korrekt fordeling.

#### *Matematisk frembragte tilfældige tal*

Ved den matematiske metode lader man regnemaskinen selv fremstille de tilfældige tal, efterhånden som der er brug for dem. Det er derfor væsentligt, at de regneoperationer, som skal udføres for at fremstille et led i rækken af tilfældige tal, er så få og simple som vel muligt, både for at spare tid og for ikke at optage for stor del af maskinen til fremstilling af tallene. Regnemaskinen skal jo, samtidig med at den fremstiller tallene, være i stand til at udføre den opgave, hvortil tallene skal bruges. Dette forhold, at man beslaglægger en del af regnemaskinens kapacitet, er en ulempe ved den matematiske metode.

Mange forskellige matematiske metoder til fremstilling af tilfældige tal har været forsøgt. Fælles for de fleste er dette, at man danner et nyt led i rækken af tilfældige tal ved at udføre

en simpel regneoperation på det foregående eller de 2 foregående tilfældige tal. Den del af regnemaskinens lager, som optages ved fremstilling af tallene, bliver på denne måde ikke så stor.

En af de ældste matematiske metoder er den såkaldte »Midsquare« metode. Man danner de enkelte tal i rækken ved at kvadrere det foregående tal og kaste de forreste og bageste cifre bort, således at antallet af cifre er konstant. Længden af perioden i de tilfældige tal fremstillet efter dette princip afhænger af startværdien. Det bedste tilfælde, man har fundet, giver en periode på  $10^6$  tal à 38 binære cifre, hvilket begrænser metodens anvendelighed.

En anden metode, som har vist sig at give bedre resultater, er *kongruens-metoden*. Den kan enten være multiplikativ eller additiv. Den multiplikative kongruensmetode er baseret på følgende udtryk

$$X_{n+1} = k \cdot X_n \text{ (modulo } M),$$

hvor modulo  $M$  angiver, at der i resultatet kun medtages de  $M$  bageste cifre. Forskellige prøver på  $M$ -cifrede tal fremstillet efter dette princip har ikke afsløret nogen form for systematik; derimod har det vist sig, at cifrene på bestemte positioner i tallene ikke udgør en tilfredsstillende serie tilfældige tal.

Den additive kongruensmetode er baseret på *Fibonacci-rækken*, som ser således ud

$$1, 1, 2, 3, 5, 8, 13, \dots, R_n, \dots$$

$$R_{n+1} = R_n + R_{n-1}$$

Modificeres rækken til følgende form

$$R_{n+1} = (R_n + R_{n-1}) \text{ modulo } M,$$

opnås en nogenlunde tilfredsstillende serie tilfældige tal. Et par led af en række udviklet på denne måde vil i det decimale talsystem se ud på følgende måde

$$\begin{array}{cccccc} 6 & 2 & 8 & 1 & 5 & \\ 3 & 1 & 4 & 7 & 9 & \\ 9 & 4 & 2 & 9 & 4 & \\ 2 & 5 & 7 & 7 & 3 & \\ 2 & 0 & 0 & 6 & 7 & \end{array} \quad M = 5$$

Med nogle mere komplicerede modifikationer af denne række har Neovius (litt. 2) ved forskellige prøver for tilfældighed opnået gode resultater. Det blev derfor besluttet at benytte tal fremstillet efter disse metoder som sammenligningsgrundlag ved vurdering af de tilfældige tal fremstillet på den senere beskrevne generator.

## Fysisk frembragte tilfældige tal

### Radioaktiv sønderdeling

Den første fysiske metode, som på laboratoriet blev forsøgt anvendt til fremstilling af tilfældige tal, var baseret på radioaktiv sønderdeling. Princippet i opstillingen, som er vist på fig. 2, er følgende:  $\gamma$ -strålerne fra et radioaktivt præparat omformes til elektriske impulser, der tilføres en tæl-

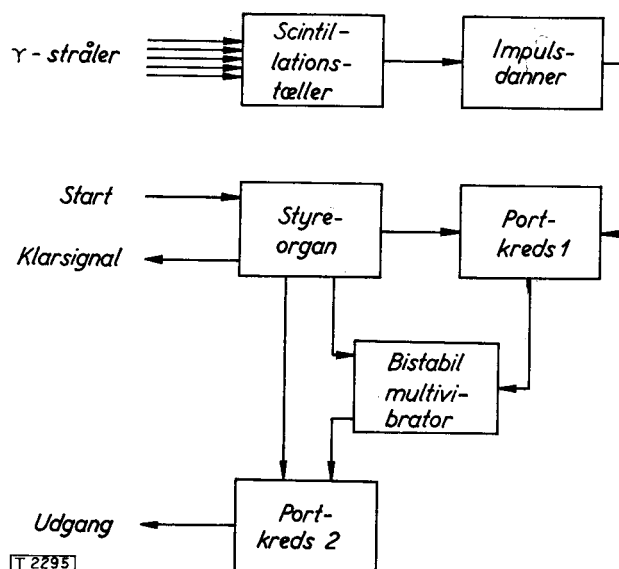


Fig. 2. Generator for tilfældige tal baseret på radioaktiv sønderdeling.

ler, som tæller antallet af impulser i et givet tidsrum. Da intervallerne mellem impulserne er tilfældigt fordelte, vil det være tilfældigt, om tælleren modtager et lige eller et ulige antal impulser i dette interval. Er antallet lige, siger vi, at udfaldet er 0; hvis antallet er ulige, er udfaldet 1. Det fremgår heraf, at tælleren kun behøver at have de to stillinger 0 og 1. En sådan binærtæller har man i den bistabile multivibrator, som er en kobling bestående af 2 elektronrør eller transistorer, og som har 2 stabile stillinger. I stilling 0 trækker det ene rør ( $t_1$ ) strøm, medens det andet ( $t_2$ ) er blokeret. I stilling 1 har rørene byttet rolle, således at  $t_1$  er blokeret, medens  $t_2$  trækker strøm. Ved en særlig indgangskobling kan man opnå, at den bistabile multivibrator skifter stilling, hver gang der tilføres en impuls til indgangen.

Koblingen på fig. 2 skal nu nærmere beskrives.  $\gamma$ -strålerne fra det radioaktive præparat omformes til elektriske impulser ved hjælp af en Scintillationstæller, som består af et organisk krystal og en fotocelle. Når  $\gamma$ -strålekvantet trænger ind i krystallet, som f. eks. kan være af nafta-

lin, vil nogle af dets atomer blive anslået og udsende lys (scintillere). Lyset opfanges af fotocellen, og den resulterende strømimpuls forstærkes og formes i impulsdanneren. Impulsen føres derefter via portkreds 1 til tælleren, en bistabil multivibrator, som afgiver udgangssignalet til portkreds 2. Hele opstillingen styres ved hjælp af et styreorgan. I hvilestillingen, når der ikke skal afgives noget tilfældigt tal, er portkreds 1 åben, således at multivibratoren står og tæller de »tilfældige« impulser. Portkreds 2 er lukket. Når der skal genereres et tilfældigt tal, sendes en startimpuls til styreorganet, som udløser følgende funktioner: Portkreds 1 lukkes, således at om-lægningen af den bistabile multivibrator standses. Via portkreds 2 aflæses multivibratorens stilling, og der gives signal til regnemaskinen om, at der er genereret et tilfældigt tal. Som afslutning nulstilles den bistabile multivibrator, inden portkreds 1 atter åbnes for de tilfældigt fordelte impulser. Det er nødvendigt at nulstille multivibratoren ved begyndelsen af hver impulsserie for at have nøjagtig de samme udgangsbetingelser for hvert tal, som genereres, da der ellers kan opstå korrelation mellem på hinanden følgende udfald.

Impulserne, som tælles af den bistabile multivibrator, har forskellige amplituder svarende til energien af de enkelte  $\gamma$ -partikler, og afstanden mellem to på hinanden følgende impulser kan blive vilkårlig lille. Da den bistabile multivibrator uundgåeligt har en vis relaxations-tid, d.v.s. at den er ufølsom over for påvirkninger i et tidsrum efter den foregående impuls, vil der fremkomme tilfælde, hvor en impuls ikke bliver talt, fordi den kommer for hurtigt efter den foregående. Denne træghed er ydermere ikke helt den samme i de to triggeretninger, ligesom følsomheden uundgåeligt er lidt forskellig i multivibratorens to stillinger. Selv om man udsøger komponenterne til den bistabile multivibrator omhyggeligt, så den bliver mest muligt symmetrisk, vil der alligevel være nogen usymmetri, og taget over længere tid vil der, efterhånden som komponenterne ældes, i de fleste tilfælde ske en forøgelse af usymmetrien. Et forsøg med opstillingen på fig. 2 viste, at denne uundgåelige usymmetri influerede mærkbart på fordelingen af 0 og 1, hvilket blev afsløret ved en simpel hyppighedsprøve. Det skal senere vises, hvorledes man ved at bruge to på hinanden følgende udfald til at generere ét tilfældigt tal er i stand til at kompensere for en sådan skævhed.

Alligevel blev tanken om at anvende radioaktiv

stråling som oprindelse for tilfældighed forladt på grund af de ret besværlige sikkerhedsforanstaltninger, som det var nødvendigt at iagttage ved omgangen med det radioaktive præparat, der skulle give en ret kraftig stråling for at opnå tilstrækkelig høj impulsfrekvens.

### Elektrisk støj

En bekvemmere og ufarligere form for tilfældige fysiske fænomener har man i elektrisk støj, enten som termisk støj i passive netværk eller som hagleffekt i elektronrør.

Den termiske støj i passive netværk skyldes, at elektronerne i de elektriske ledere i overensstem-

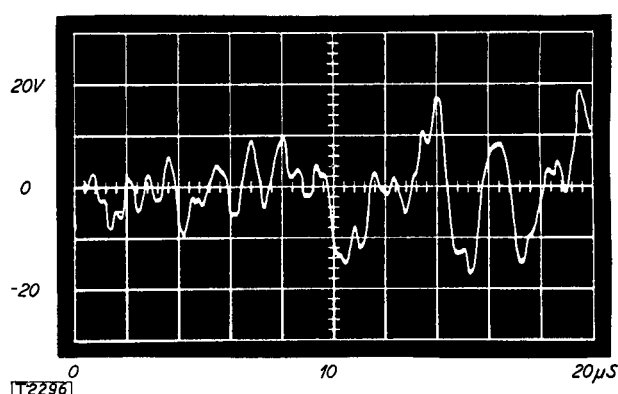


Fig. 3. Støjspænding efter støjforstærker.

melse med den kinetiske teori har tilfældigt fordelte hastigheder, hvis middelværdi afhænger af den absolutte temperatur. Hagleffekten i elektronrør skyldes kvantiseringen i elektronemissionen fra glødekathoden, og at de enkelte elektroner emitteres fra katoden med tilfældigt fordelte tidsintervaller. Anodestrømmen vil derfor få tilfældige variationer. Fig. 3 viser som eksempel støjspændingen fra en diode, efter at den er forstærket i en forstærker med ca. 400 kHz øvre grænsefrekvens. Af de to støjformer er rørstøjen fordelagtigst, da den er kraftigere end den termiske støj og følgelig kræver mindst forstærkning.

Det skal nu vises, hvorledes det er muligt at danne tilfældige tal ud fra støjspændingen. Der er flere muligheder, men de følgende to principper antages at være repræsentative for dem alle.

Ved den første metode, *summationsmetoden*, tælles antallet af gange, som støjspændingen skærer nullinien i opadgående retning inden for et fast tidsinterval. Hvis antallet er lige, kaldes udfaldet 0, hvis det er ulige, 1. Det fastsatte tidsinterval må være stort i forhold til periodelængden af den højeste frekvenskomponent i støjen, for at tallene kan blive tilfældige.

Den anden metode er *udlæsemetoden*. Her udlæses støjspændingens fortegn med regelmæssige intervaller. Støjspændingen er efter forstærkningen en ren vekselspænding som varierer omkring 0. Længderne af intervallerne mellem nulgennemgangene er tilfældige og fordeler sig efter en eksponentiel fordeling, d.v.s. det er tilfældigt, om støjspændingen til udlæsetidspunktet er positiv eller negativ, hvis udlæsefrekvensen er lille i forhold til den øvre grænsefrekvens i støjforstærkeren.

De to metoder er principielt lige gode, men af rent praktiske grunde er udlæsemetoden bedst egnet til formålet. Det blev derfor besluttet at konstruere en generator for tilfældige tal baseret på denne metode med en diode som kilde for støjspændingen. Princippet i opstillingen er vist på fig. 4. Støjspændingen forstærkes og omdannes til en firkantspænding, som har værdien 0 V, når støjspændingen er positiv, og  $-10$  V, når støjspændingen er negativ. Udlæsningen af støjspændingens fortegn sker i en portkreds ved hjælp af en række udlæseimpulser, som kommer med  $50 \mu\text{s}$  mellemrum. Når støjspændingen er negativ til udlæsetidspunktet, er firkantspændingen også negativ, og portkredsen vil være blokeret for udlæseimpulsen. Hvis støjspændingen er positiv, er firkantspændingen 0, og portkredsen vil være åben, således at udlæseimpulsen kan passere portkredsen og trigge den monostabile multivibrator. Denne er en kobling bestående af to trioder eller transistorer, som har én stabil stilling. Triggres den med en impuls, vil den skifte over til sin ustabile stilling og forblive der i en tid, som er bestemt af kredsens dimensionering, og derefter selv falde tilbage til den stabile stilling. Udgangsspændingen fra multivibratoren er 0 V i hvilestillingen og  $-20$  V i den ustabile stilling. Hvis udgangsspændingen fra den monostabile multivibrator er 0 V umiddelbart efter udlæseimpulsen, betyder det, at støjspændingen var negativ på udlæsetidspunktet, og tilsvarende vil udgangsspændingen lige efter udlæseimpulsen være negativ, dersom støjspændingen var positiv på udlæsetidspunktet. De to mulige udgangsspændinger svarer til de binære tal 0 og 1.

Da de kredse, som vi må arbejde med, ikke er ideelle, vil man med den simple opstilling, som er vist i fig. 4, få en vis usymmetri i udfaldene 0 og 1. Det væsentligste bidrag til denne usymmetri opstår ved omdannelsen af støjspændingen til en firkantspænding. Vi skal se lidt nærmere på årsagerne til dette forhold.

Firkantgeneratoren består af en Schmitt-trigger, som er en bistabil kobling bestående af to rør. I denne henseende ligner den den bistabile multivibrator, men medens den sidstnævnte skifter stilling, hver gang den påtrykkes en impuls, vil den ideelle Schmitt-trigger skifte stilling, hver gang indgangsspændingen skifter fortegn. Når

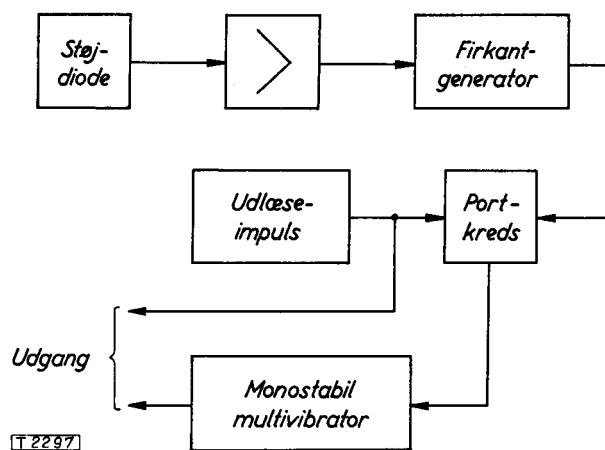


Fig. 4. Princip for udlæsemetoden.

den påtrykte spænding er negativ, står Schmitt-triggeren i sin ene stabile stilling, og når den er positiv, vil Schmitt-triggeren stå i den anden stilling uafhængigt af spændingens størrelse i øvrigt. Schmitt-triggeren vil altså kun skifte stilling, når indgangsspændingen passerer nulniveauet.

Dette nulniveau afhænger imidlertid af forskellige komponentværdier og rørparametre på en sådan måde, at det er umuligt at fastlægge det eksakt eller at holde det konstant, uafhængigt af ældning. En forskydning af nulniveauet i f. eks. positiv retning vil direkte bevirke en ændring i firkantspændingen, således at den tid, hvor den er negativ, i middel bliver længere, medens den tid, hvor den er 0, bliver kortere. Dette fremgår tydeligt af fig. 3. Sandsynligheden for, at firkantspændingen er negativ på udlæsetidspunktet, bliver følgelig større end  $\frac{1}{2}$ . Den uundgåelige usymmetri vil altså bevirke en skævhed i udfaldene 0 og 1. Det er derfor nødvendigt at udbygge princippet fra fig. 4.

Udfaldet af udlæsningen kaldes + og –, svarende til at støjspændingen er positiv henholdsvis negativ på udlæsetidspunktet. Hvis sandsynligheden for udfaldet + er  $\frac{1}{2} + \delta$ , da er sandsynligheden for udfaldet – lig med  $\frac{1}{2} - \delta$ . For at fjerne denne skævhed indføres dobbeltspil, således at udfaldet af to på hinanden følgende udlæsninger bruges til at generere ét tilfældigt tal.

Sandsynligheden for at få udfaldene (+ —) efter hinanden er

$$P(+ -) = (\frac{1}{2} + \delta) (\frac{1}{2} - \delta) = \frac{1}{4} - \delta^2$$

Vi kalder dette udfald 1. Sandsynligheden for at få udfaldene (— +) er

$$P(- +) = (\frac{1}{2} - \delta) (\frac{1}{2} + \delta) = \frac{1}{4} - \delta^2$$

og udfaldet kaldes 0. Man ser at  $P(+ -) = P(- +)$ . Udfaldene (+ +) og (— —), der har sandsynlighederne  $(\frac{1}{2} + \delta)^2$  henholdsvis  $(\frac{1}{2} - \delta)^2$ , kasseres.

Hvis  $\delta$  er konstant, hvilket kan forudsættes, har man opnået symmetri i udfaldene 0 og 1 på bekostning af den hastighed, hvormed tallene genereres. Antallet af producerede tilfældige tal bliver  $\frac{1}{4}$  af antallet af udlæsninger, idet udfaldet af udlæsningerne parres to og to, og halvdelen af parrene kasseres.

Ved at indføre dobbeltspil har vi altså opfyldt den ene af de to nødvendige betingelser, som tallene skal opfylde for at være tilfældige. Den anden betingelse er, at der ikke må være nogen sammenhæng eller korrelation mellem tallene. En talrække, hvor sandsynligheden er  $\frac{1}{2}$  for de 2 mulige udfald, men som har en kraftig korrelation, kan f. eks. se således ud: 1—0—1—0—1—0 o. s. v. Det må derfor undersøges, om der kan opstå nogen korrelation i opstillingen, som benyttes.

Støjen fra støjdioden er såkaldt hvid støj, d. v. s. dens spektrum indeholder alle frekvenser inden for et meget bredt frekvensområde med samme amplitude for alle komponenter. Hvis støjen blev forstærket i en forstærker med en meget lille båndbredde, ville det, vi fik ud af forstærkeren, være en næsten ren sinussvingning med en frekvens midt i forstærkerens gennemgangsområde. Den forstærkede støjspænding er i dette tilfælde meget lidt tilfældig, idet alle intervallerne mellem nulgennemgangene har næsten samme længde. På den anden side er det umuligt at lave en forstærker med uendelig stor båndbredde. Det er derfor nødvendigt at finde sammenhængen mellem korrelation og frekvenskarakteristik for at fastlægge de krav, vi skal stille til forstærkeren.

På grundlag af autokorrelationsfunktionen

$$\psi(\tau) = X(t) \cdot X(t + \tau),$$

hvor  $X(t)$  er en funktion, som har værdien + 1, når støjspændingen er positiv, og — 1, når støjspændingen er negativ, og hvor  $\tau$  er lig afstanden

mellem udlæseimpulserne, kan man opstille et udtryk for korrelationen i støjen, efter at den har passeret forstærkeren (litt. 6, side 317). Ud fra dette udtryk bestemmes den nødvendige båndbredde for en given  $\tau$  og en given form af frekvenskarakteristikken og med en maksimal tilladelig korrelation. For de i den færdige generator anvendte data, nemlig udlæseperiode  $\tau = 50 \mu\text{s}$  og forstærkerbåndbredde  $B = 330 \text{ kHz}$  (70 kHz — 400 kHz) og RC-afskæring, bliver den normerede autokorrelation

$$\psi(\tau)_0 = 3 \cdot 10^{-65},$$

d. v. s. forsvindende lille.

De øvrige elementer i opstillingen på fig. 4: Firkantgeneratoren, portkredsen og den monostabile multivibrator giver ikke anledning til tilsvarende teoretiske overvejelser. Ved omhyggelig dimensionering og rigelige marginaler kan man sikre sig, at der ikke opstår korrelation mellem på hinanden følgende udfald i disse led.

#### Opbygning af generator for tilfældige tal

Generatorens opbygning og funktion vil fremgå af følgende gennemgang af blokskema og impulsdiagram (fig. 5 og 6).

Støjspændingen føres fra støjdioden gennem forstærkeren via en katodefølger  $KF$  1 til en Schmitt-trigger, som omdanner støjspændingen til en firkantspænding (6) (Tallene i parentes refererer til impulsdiagrammet). Dette signal, som varierer mellem 0 og —10 V, tilføres portkreds (gate)  $G$  1 via en katodefølger  $KF$  2.  $G$  1 tilføres desuden udlæseimpulsen (5) fra en impulsdanner, som trigges af impulserne (4) fra en fritløbende blokeringsoscillator, hvis frekvens er 20 kHz.

$G$  1 er en heptode,  $E$  91  $H$ , med to styregitre, to skærmgitter og ét fanggitter. Firkantspændingen tilføres det ene styregitter og udlæseimpulsen det andet. Kun når støjspændingen er positiv på udlæsetidspunktet, og firkantspændingen altså er 0, vil røret overføre udlæseimpulsen. Denne impuls trigger via en katodefølger  $KF$  3 den monostabile multivibrator  $M$  2, som afgiver en impuls (8) på 30  $\mu\text{s}$  varighed, d. v. s. kortere end afstanden mellem udlæseimpulserne.  $M$  2 bliver altså kun trigget, når støjspændingen er positiv på udlæsetidspunktet.

Som tidligere beskrevet anvendes to på hinanden følgende udlæsninger til at generere ét tilfældigt tal. Udfaldet af en udlæsning må følgelig opbevares i en hukommelse, indtil udfaldet af





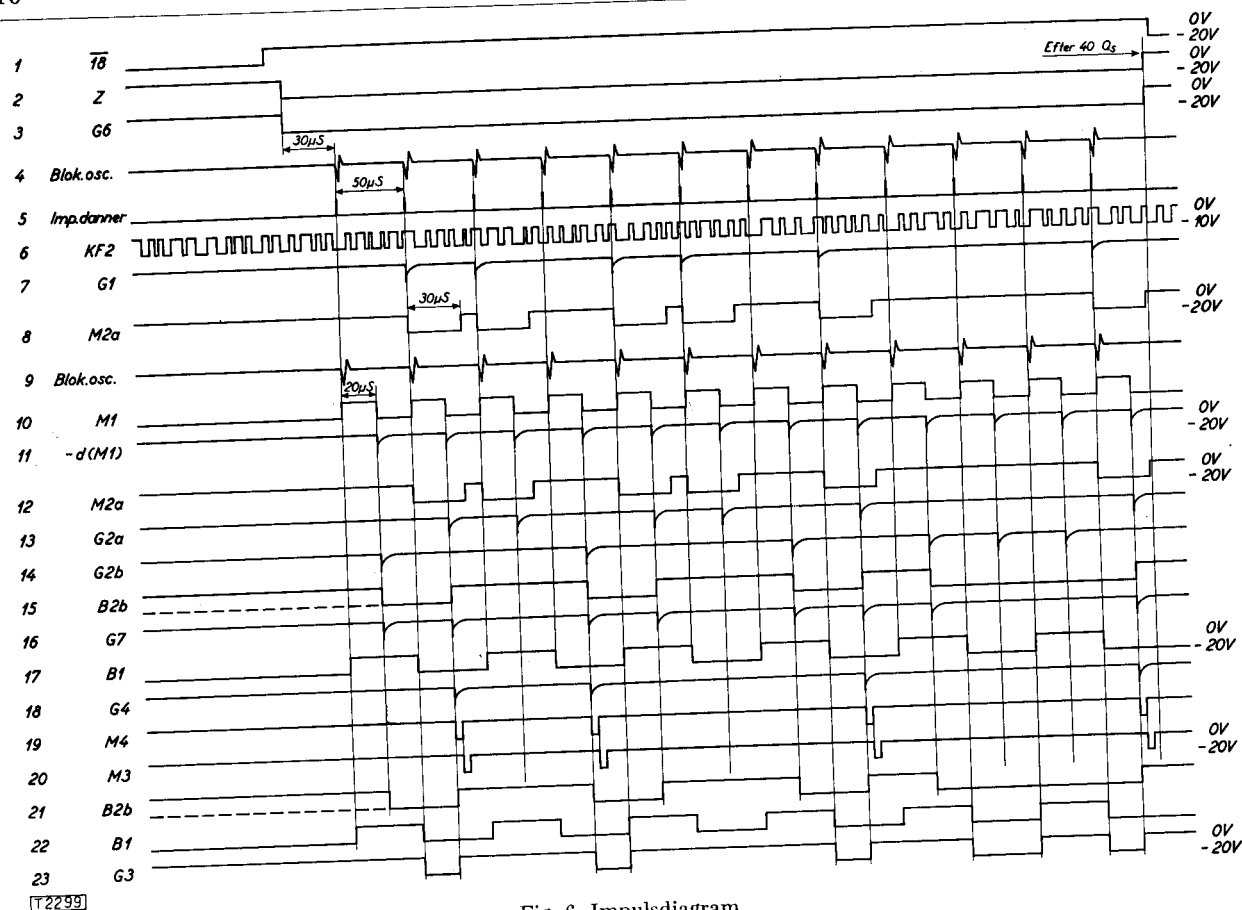


Fig. 6. Impulsdiagram.

lukket for impulsen fra  $M1$  (13), således at  $B2$  bliver trigget til stilling 1.

$B2$  skifter følgende stilling, hver gang et udfald af støjspændingsudlæsningen har modsat fortegn af det foregående, medens den forbliver, når udfaldet ikke skifter fortegn. Det betyder, at man får et positivt spring (15) på den ene udgang  $b$  af  $B2$ , når støjspændingen udlæses som positiv efter at have været negativ ved foregående udlæsning, udfald ( $- +$ ), og et positivt spring på den anden anode  $a$  af  $B2$ , når udfaldet er ( $+ -$ ). De to anodespændinger fra  $B2$  differentieres, og de positive impulser føres til en »eller«-portkreds  $G7$ , som giver et udgangssignal (16), når der er signal på enten den ene eller den anden af de to indgange, d.v.s. hver gang  $B2$  lægger om.

Resultatet af udlæsningerne skal kombineres to og to, men på en sådan måde, at parrene ikke overlapper. Til dette formål indføres en portkreds  $G4$ , som styres af den bistabile multivibrator  $B1$ .  $B1$  trigges af blokeringsoscillatoren og lægges om ved hver impuls, således at  $G4$  er åben i hvert andet interval mellem impulserne (17). Fra  $G4$  kommer følgende en impuls (18), hver gang der foreligger et isoleret udfaldspar ( $+ -$ ) eller ( $- +$ ). Udfaldet af det tilfældige tal bestemmes ved at

kombinere signalet fra  $B1$  med signalet på den ene udgang af  $B2$  i portkredsen  $G3$ . Hvis signalet fra  $G3$  (23) er negativt ( $-20V$ ), når der kommer en impuls fra  $G4$ , er det tilfældige tal 0, og hvis signalet fra  $G3$  er 0 V, er det tilfældige tal 1. Da signalet fra  $G3$  (23) skifter samtidigt med forkanten af impulsen fra  $G4$  (18), er det nødvendigt at forsinke denne impuls for at få en veldefineret spænding på  $G3$  til bestemmelse af udfaldet af det tilfældige tal. Forsinkelsen sker i den monostabile multivibrator  $M4$ , som trigger en anden monostabil multivibrator  $M3$ , der giver den egentlige udgangsimpuls  $Q_s$  (20) via  $KF6$ .

Fra  $M3$  får vi således en negativ impuls (20) på ca.  $5\mu s$  længde, hver gang der foreligger et tilfældigt tal, og udfaldet af det tilfældige tal bestemmes af fortegnet af signalet fra  $G3$ . De tilfældige tal tilføres regnemaskinen i form af disse to signaler.

Når regnemaskinen (DASK) er klar til at modtage en serie tal, sendes to signaler til generatoren. Først afgives ordren  $\overline{18}$  (1) og lidt senere startsignalet  $Z$  (2). Disse signaler kombineres i portkredsen  $G6$ . Fra  $G6$  har man i hvilestillingen (når der ikke skal sendes tal til DASK) 0 V (3), og i arbejdsstillingen  $-20V$ , som åbner  $G5$  for

de negative impulser fra *M 4*. Signalet fra *G 6* (3) styrer desuden blokeringsoscillatoren, således at denne normalt er standset (4). Først ved klar-signal fra DASK ophører blokeringen, og den første udlæseimpuls kommer ca. 30  $\mu$ s senere.

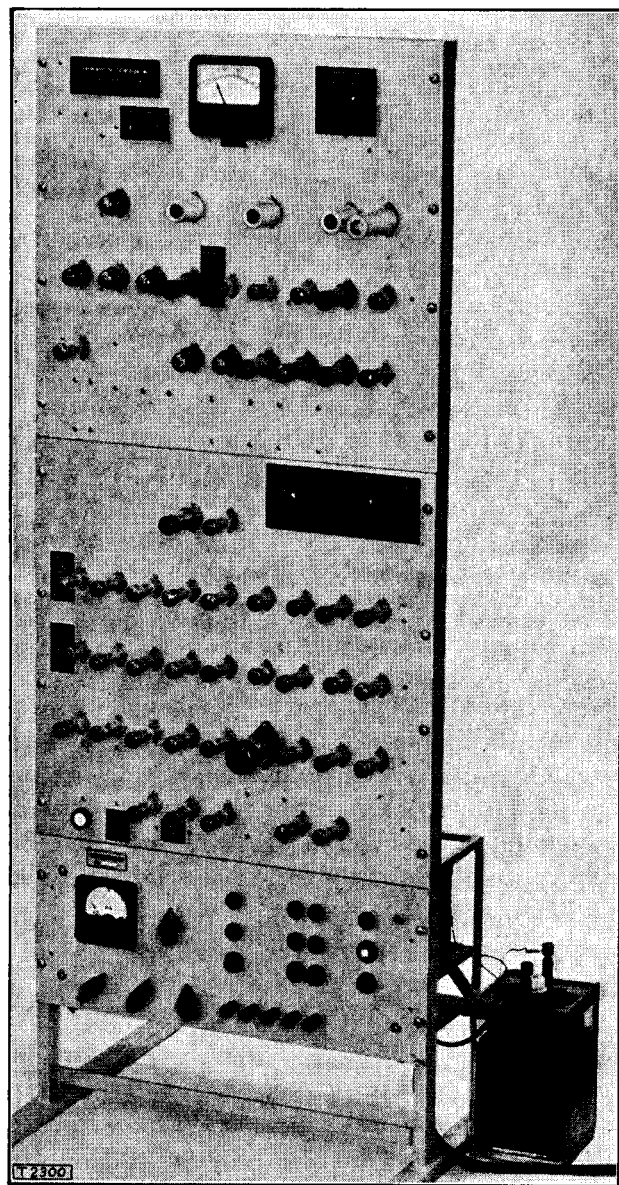


Fig. 7. Generator for tilfældige tal.

Ved denne synkronisering undgår man fejl ved overføringen af det første tal i en serie.

De tilfældige tal skal afgives til DASK i serier på 40, da DASK arbejder med 40-cifrede tal. Der er derfor indbygget en tæller bestående af de to bistabile multivibratorer  $B_3$  og  $B_4$  samt en dekadetæller ( $E1T$ ), som tæller  $Q_s$ -impulserne. For hver 40  $Q_s$ -impulser sendes én impuls ( $j$ ) til DASK, som bevirker, at  $Z$ -spændingen forsvinder, udlæsningen standser, og produktionen af en cifferserie ophører.

### Generatorens praktiske opbygning

Konstruktionen af alle de anvendte kredse, monostabile og bistabile multivibratorer, portkredse, Schmitt-trigger, blokeringsoscillator, o.s.v. er foretaget efter almindeligt kendte principper (se f. eks. litt. 7). Dimensioneringen blev udført med samme tolerancer, som normalt anvendes ved opbygning af regnemaskinekredsløb. Kredsene kan fungere korrekt for ændringer af modstandsværdier på  $\pm 10\%$  og mindskelse af rørens emission til det halve.

På fig. 7 ses den fremstillede generator i den endelige udformning. Monteringen er udført i et 19 tommer standardstel på 3 chassisplader. Der er i alt medgået 55 rør til opstillingen (ekskl. rør til spændingsforsyninger) fortrinsvis af typerne *E 90 CC*, *E 80 L* og *E 180 F*.

Støjdioden (*K 81 A*) med tilhørende forstærker er placeret øverst på stellet, for at afskærmningen kan blive så effektiv som muligt. Støjforstærkeren har i frekvensområdet 70–400 kHz en forstærkning på 50 000 gange (94 dB), og støjniveauet reguleres ved at ændre glødestrømmen i støjdioden. Da det er væsentligt, at støj-spændingen ikke kommer under et vist niveau, er der i stellet anbragt et diodevoltmeter, som direkte viser støjniveauet. På øverste plade er desuden anbragt Schmitt-triggeren samt *G 1* og *M 1*. Alle de logiske kredse er samlet på midterste plade, medens den nederste plade optages af en stabiliseret spændingsforsyningsenhed, som forsyner alle de følsomme kredse på den øverste plade. De øvrige kredse spændingsfødes fra DASK. Glødespændingen til støjdioden fås fra en 2 V akkumulator.

På stelletts forside findes en række målebøsninger til brug ved justering og kontrolmålinger, ligesom der er indbygget et kontrolorgan, hvormed de logiske kredses funktion kan kontrolleres. En normal start af generatoren kræver dog ikke nogen justering og sker ved at slutte netafbryderen og skrue op for glødestrømmen i støjdioden.

### Resultater af undersøgelser af tilfældige tal

De af generatoren fremstillede tilfældige tal blev underkastet en serie omfattende statistiske undersøgelser. Alle de anvendte prøver, som er beskrevet i et tidligere afsnit, blev udført på DASK. De detaljerede undersøgelsesresultater vil blive udførligt refereret i en særlig rapport. Her skal blot anføres, at det med de anvendte statistiske prøver ikke var muligt at afsløre nogen form

for systematik i de tilfældige tal, frembragt af den konstruerede generator.

Som et eksempel på en enkelt af undersøgelserne er på **fig. 8** vist resultatet af en hyppighedsprøve på  $2 \cdot 10^7$  binære cifre.

Til sammenligning blev et antal serier af tilfældige tal, frembragt efter to forskellige matematiske metoder (litt. 2 side 282, metode (3) og (4.1)), underkastet de samme undersøgelser. Disse undersøgelser viste, at de anvendte matematiske metoder ikke gav fuldstændigt tilfældige tal, idet et par af prøverne afslørede systematik i tallene. Den konstruerede generator må derfor anses for det bedste til rådighed stående middel til fremstilling af tilfældige tal.

### Slutning

Med afslutningen af dette projekt er der skabt mulighed for udførelse af beregninger efter Monte Carlo-metoden på DASK, og man har derfor — på foranledning af ATU's trafikmaskineudvalg — på Regnecentralen påbegyndt udviklingen af en kode til løsning af graderingsopgaver på DASK.

Det første forsøg på at anvende Monte Carlo-metoden ved trafikundersøgelser af graderinger, der er foretaget inden for de danske telefon-administrationer, blev udført i 1954 af civilingeniør Carl Jacobsen, JTAS, (TT 1954, side 260). Dette forsøg blev udført efter analogimaskineprincippet. Som det tidligere er nævnt, er de elektroniske cifferregnemaskiner imidlertid i flere henseender bedre egnede til løsning af denne type opgaver, og efter at beslutningen om at bygge DASK var truffet, anbefalede trafikmaskineudvalget, at man baserede sig på anvendelsen af denne maskine, og at der skulle fremstilles en særlig generator til frembringelse af tilfældige tal.

Udviklingen af generatoren for tilfældige tal er udført på Teleteknisk Forskningslaboratorium under ledelse af professor J. Oskar Nielsen med økonomisk støtte fra Marshall-midlerne i henhold til lov nr. 209 af 7/6 1952.

Arbejdet hermed blev påbegyndt af Regnecentralens tekniske leder, civilingeniør B. Scharøe-Petersen, som udførte en række forsøg med an-

vendelsen af radioaktiv sønderdeling som kilde for tilfældighed. De sandsynlighedsteoretiske overvejelser, som ligger til grund for denne opstilling, skyldes Regnecentralens direktør, N. I. Bech. Kodningen af programmerne for de matematiske

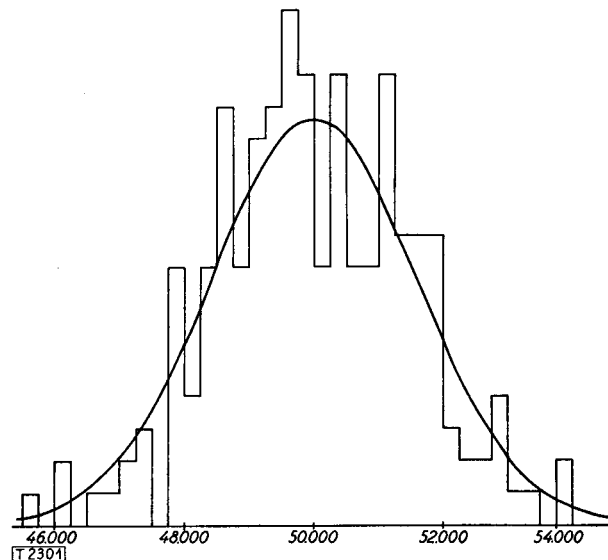


Fig. 8. Fordelingskurve for fysisk frembragte tal. Trappekurven viser den relative hyppighed af udfaldet 0 i 200 serier à  $10^5$  binære cifre. Til sammenligning er indtegnet den teoretiske normale fordelingskurve.

frembragte tilfældige tal og for de benyttede prøver for tilfældighed er udført på Regnecentralen af cand. polit. Å. Melbye, ligesom alle de statistiske undersøgelser er udført på Regnecentralen. Forfatteren ønsker gerne på forskningslaboratoriets vegne at takke alle, som har medvirket ved udviklingen af dette projekt.

### Litteraturliste

1. E. Brockmeyer, Sandsynlighedsregningens anvendelse i telefonteknikken, TT 1952, side 95.
2. G. Neovius, Artificial Traffic Trials Using Digital Computers, Ericsson Technics 1955, nr. 2, side 280.
3. J. Rybner, Teorien for elektriske kredsløb og ledninger, Den private ingeniørfond 1952.
4. Kendall and Smith, Tables of Random Sampling Numbers, Tracts for Computers XXIV, Cambridge 1951.
5. N. A. Arley og K. Rander Buch, Sandsynlighedsregning, G. E. C. Gad 1950.
6. Van der Ziel, Noise, Chapman and Hall Ltd, London 1955.
7. Millman and Taub, Pulse and Digital Circuits, Mc Graw-Hill Book Comp. London 1956.